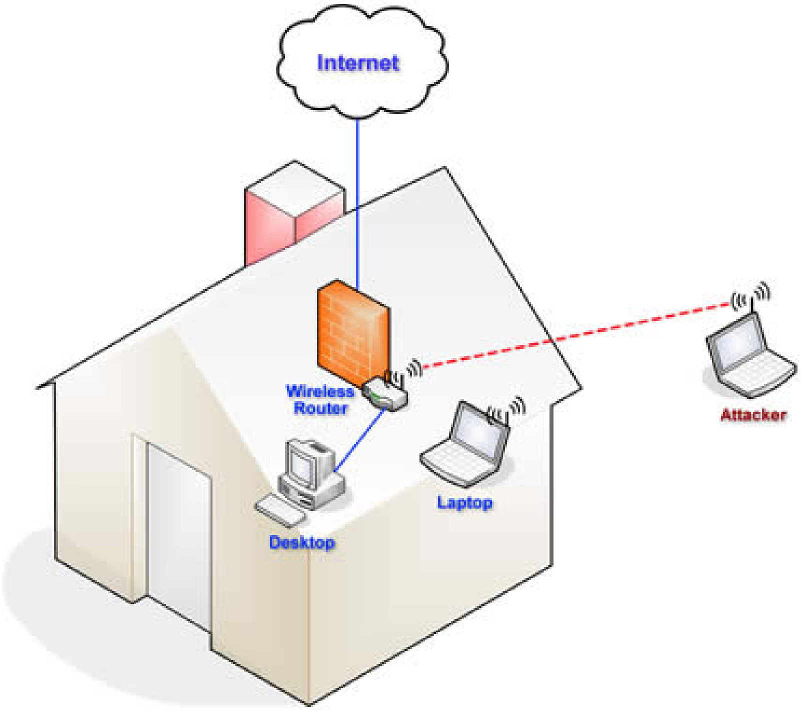
WIRELESS **SECURITY**

How to protect yourself from unknown wireless security treats and hacking attempts.

Overview

This article contains helpful tips on protecting youself against wireless security threats, and inform you of the common features available in today's wireless routers and access points. When properly used, these features will give you an enhanced level of security and greater peace of mind.



Is Your Wireless Network Secure?

Most people are eager to setup their wireless home networks and often rush through the job in order to get connected with the Internet as quickly as possible. Unfortunately, this can leave you vulnerable to attacks because most manufacturers ship their wireless devices with security features completely turned off. They do this because configuring security settings can be tedious and non-intuitive. Therefore, it is important to understand how this makes you vulnerable to an attack, and what steps you need to take to protect yourself.

Wireless network devices send and receive radio signals that broadcast through the air, which can make the signal easy to intercept by others. Signals passing through your home's exterior walls can be intercepted by your neighbor, or anyone that is within reasonably close proximity to your home.

You have to consider the possibility that an intruder could spy on your communications, steal your identity, or even destroy valuable information stored on your home network.

Are You Safe from Attackers?

Unknown by you, someone could exploit your wireless Internet connection to perform illegal or malicious acts while hiding anonymously behind your connection. These acts could eventually be traced back to you by authorities who have identified your network as their source.

There Are Ways You Can Protect Yourself

Although this sounds threatening, wireless routers and access point can be relatively safe to use because there are ways to protect yourself and if you follow some of the steps below, you will substantially increase your security and peace of mind:

1. Change the username and password. Most routers have a default username and password that are easy to determine because they are published on the Internet. Change these settings immediately.

2. Turn on WAP/WEP Encryption. All Wi-Fi equipment supports some form of "encryption." Encryption technology scrambles information sent over wireless networks so that they cannot be easily read by outside parties. There are several encryption technologies, so you will want to pick the strongest form of encryption available on your network.

3. Change the SSID name. All access points and routers use a network name called the Short Service Set Identifier, or SSID. Most manufacturers ship their products with the same SSID set. Changing the default SSID to something unique will make your router or access point less identifiable.

4. Turn off SSID. With wireless networking, an access point or router typically broadcasts the network name (SSID) over the air. Typically, this feature is unnecessary, and it increases the likelihood an unwelcome neighbor or hacker will try to log in to your home network.
5. Turn the network off. If you plan on being away from your home for an extended period, turning your equipment off is the best form of protection.

6. Every network device has a unique identifier called a MAC address, access points and routers keep track of the MAC addresses of all devices that connect to them. Many give you the option to enter the MAC addresses of your home network equipment that connects to them. This restricts the network to others by filtering out all other devices other than the connections from the devices you enter. Although this is an important feature, a good Hacker can easily fake a MAC address.

7. Most home network devices use dynamic IP addresses, or DHCP, which makes it easy to connect devices but, unfortunately, this convenience also allows network attackers to easily obtain IP addresses from a network. Turn off DHCP, and then set a fixed IP address range and set each connected device to match. Use a private IP range, such as 10.0.0.x. This will prevent computers from being directly available from the Internet.

For more comprehensive information, carefully review the security settings of you wireless device's manual, or contact the manufacturer's technical support service. Although it can be challenging to get your wireless device configured correctly, it will give you piece of mind knowing that you have implemented to best protection feature available to you.

Useful Links

Security Practicum: Essential Home Wireless Security Practices

Complete Guide to Wi-Fi Security

eSecurity Planet.com